PETIR

JURNAL
PENGKAJIAN DAN PENERAPAN
TEKNIK INFORMATIKA

VOLUME 9 - NOMOR 1 | MARET 2016 | ISSN 1978-9262

PENENTUAN NASABAH PENERIMA REWARD PRODUK *GOLD* DENGAN METODE *SIMPLE ADDITIVE WEIGHTING* (SAW) STUDI KASUS : PT. PINJAM INDONESIA
Riki Ruli A. Siregar; Faizal Fachrurrozi

IMPLEMENTASI METODE *BACKWARD CHAINING* PADA DATA *WAREHOUSE* DAOP 1 JAKARTA PT. KAI (PERSERO)
Rakhmat Arianto; Chandra Bagus Sugiarto

IMPLEMENTASI METODE DETEKSI TEPI *CANNY* PADA OBJEK SEBAGAI MODEL KEAMANAN APLIKASI PADA SMARTPHONE ANDROID
Abdul Haris; Andi Prasetyo

ANALISA DATA DAN PERANCANGAN APLIKASI SERVICE PELANGGAN PT. JNE UNTUK PENINGKATAN KUALITAS LAYANAN
Dewi Arianti Wulandari; Sonny Syahrindra Putra

JARINGAN AD-HOC VEHICULAR (VANET) : TINJAUAN TENTANG ARSITEKTUR, KARAKTERISTIK, APLIKASI, DAN PROTOKOL *MEDIUM ACCESS CONTROL* (MAC)
Rosida Nur Aziza

PERANCANGAN APLIKASI PENJADWALAN MATA KULIAH MENGGUNAKAN METODE *CONSTRAINT PROGRAMMING*
Syam Gunawan

RANCANGAN TATA KELOLA PEREMAJAAN RUANG KELAS DIREKTORAT PEMBINAAN SEKOLAH DASAR
Ratna Mutu Manikam; Purwanto

PENGEMBANGAN AMORIK MENGGUNAKAN METODE GARIS SINGGUNG TERHADAP DUA LINGKARAN DAN PERSAMAAN KURVA BEZIER ORDE DUA.
Darma Rusjdi

OPTIMALISASI PENGAMBILAN KEPUTUSAN PENILAIAN KINERJA DOSEN PADA PERGURUAN TINGGI ISLAM XYZ MENGGUNAKAN AHP (ANALYTICAL HIERARCHY PROCESS)
Rahma Farah Ningrum

PENGAMANAN SMS PADA TELEPON SELULER BERBASIS ANDROID MENGGUNAKAN ALGORITMA TRIPLE DES
Raka Yusuf; M. Rival Suheri

APLIKASI LATIHAN SOAL UJIAN TEORI SURAT IZIN MENGEMUDI BERBASIS WEB
Harni Kusniyati; Raka Yusuf; Andri Setiawan

RANCANG BANGUN SIMULASI TERJADINYA LISTRIK DENGAN SUMBER DAYA SAMPAH BERBASIS MULTIMEDIA (STUDI KASUS : TPST BANTAR GEBANG)
Yasni Djamain; Ika Fitriyani Putri

ISSN 1978-9262
771978 926272

SEKOLAH TINGGI TEKNIK - PLN (STT-PLN)

PETIR	VOL. 9	NO. 1	HAL. 1 - 87	JAKARTA, MARET 2016	ISSN 1978-9262

PENGAMANAN SMS PADA TELEPON SELULER BERBASIS ANDROID MENGGUNAKAN ALGORITMA *TRIPLE DES*

Raka Yusuf; M. Rival Suheri
Program Studi Sistem Informasi Fasilkom Universitas Mercu Buana
raka@mercubuana.ac.id; reeeval@gmail.com

ABSTRAK

Salah satu fasilitas yang disediakan telepon seluler untuk melakukan pengiriman data berupa pesan singkat yaitu melalui SMS (Short Message Service). Seiring dengan perkembangan teknologi tersebut, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin menyimpan suatu informasi rahasia dengan menyimpan pesan SMS. Secara umum penyimpanan pesan SMS tidak menjamin kerahasiaan pesan yang disimpan oleh pengguna. Sebuah informasi umumnya hanya ditujukan bagi segolongan tertentu. Oleh karena itu sangatlah penting untuk mencegahnya agar tidak jatuh kepada pihak-pihak yang tidak berhak. Untuk keperluan tersebut, maka diperlukan sebuah teknik kriptografi dengan metode enkripsi dan dekripsi pesan. Dengan memanfaatkan algoritma kriptografi Triple DES, penulis membuat suatu aplikasi pengiriman pesan secara tersandikan pada telepon seluler yang berbasis android untuk mengamankan suatu informasi yang disimpan atau yang dikirimkan oleh pengguna. Metode yang digunakan dalam membangun aplikasi ini yaitu Metode Waterfall. Metode dimulai dari pendefinisian kebutuhan lalu analisa, desain, implementasi, pengujian dan pemeliharaan aplikasi. Dengan adanya aplikasi pengenkripsian pesan ini diharapkan pengguna dapat mengirimkan atau menyimpan suatu informasi rahasia tanpa takut diketahui isi informasi tersebut oleh orang lain.

***Kata Kunci**: Kriptografi, Triple DES, Enkripsi, Keamanan Data, SMS, Android*

1. PENDAHULUAN

1.1 Latar Belakang

Pada perkembangan teknologi informasi yang semakin maju, kebutuhan manusia akan sarana informasi semakin bertambah. Namun hal itu seringkali terhambat oleh masalah-masalah seperti jarak, mobilitas, dan keamanan data. Telepon seluler memungkinkan seseorang berkomunikasi dengan jarak jauh. Dengan kecanggihan teknologi saat ini, fungsi telepon seluler tidak hanya sebagai alat komunikasi biasa, tetapi juga dapat mengakses internet, memotret gambar/merekam video dan juga saling mengirim data. Salah satu fasilitas yang disediakan telepon seluler untuk melakukan pengiriman data berupa pesan singkat yaitu melalui SMS (*Short Message Service*). Walaupun merupakan bagian dari kemampuan standard GSM fase pertama, SMS masih merupakan layanan yang banyak digunakan oleh masyarakat.

Seiring dengan perkembangan teknologi tersebut, timbul pertanyaan mengenai keamanan informasi jika seseorang ingin menyimpan suatu informasi rahasia dengan menyimpan pesan SMS. Secara umum penyimpanan pesan SMS tidak menjamin kerahasiaan pesan yang disimpan oleh pengguna. Sehingga dibutuhkan suatu sistem keamanan dalam menyampaikan dan menyimpan pesan tersebut.

Celah keamanan pada komunikasi via SMS adalah pesan yang dikirimkan akan disimpan di SMSC (*Short Message Service Center*), yaitu tempat dimana SMS disimpan sebelum dikirim ke tujuan. Ketika kita mengirimkan pesan, maka pesan tersebut disampaikan ke suatu sistem komputer yang mungkin kita tidak mengetahui administratornya.

Pesan yang sifatnya *plaintext* (teks-terang) ini dapat dibaca oleh siapa saja yang berhasil memiliki akses ke dalam SMSC, atau misalkan telepon seluler kita dipinjam atau hilang/dicuri, sehingga orang lain bisa melihat informasi-informasi penting yang ada didalamnya. Akibatnya, informasi penting seperti informasi rahasia, password, nomer pin, dan lain-lain dapat dibaca oleh orang yang tidak berhak untuk mengetahuinya. Kerahasiaan pesan SMS terancam bukan oleh para hacker, melainkan para administrator sistem itu sendiri atau orang lain yang meminjam dan menemukan/mencuri telepon seluler tersebut.

Pada tugas akhir ini, penulis akan mengimplementasikan paket kriptografi yang disediakan oleh Java dan membuat sebuah aplikasi pengamanan SMS dengan menggunakan metode Triple DES untuk mengenkripsi data yang dikirimkan melalui SMS pada sistem operasi android sehingga pemilik handphone yang berbasis android dapat melakukan pengiriman pesan dengan lebih aman.

2. LANDASAN TEORI

2.1 Kriptografi

Kriptografi didefinisikan sebagai ilmu dan pelajaran untuk tulisan rahasia dengan pertimbangan bahwa komunikasi dan data dapat

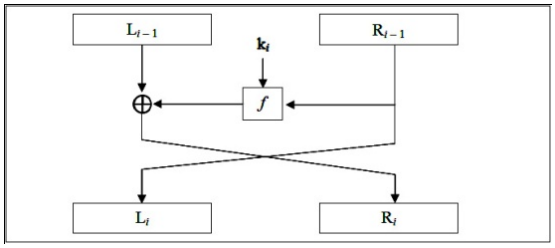
dikodekan untuk mencegah dari mata-mata atau orang lain yang ingin mengetahui isinya, dengan menggunakan kode-kode dan aturan-aturan tertentu dan metode lainnya sehingga hanya orang yang berhak yang dapat mengetahui isi pesan sebenarnya. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. (Menezes, A. dkk, 1996:4).

2.2 Triple DES

Triple DES (*Triple Data Encryption Standard*) atau TDES adalah salah satu algoritma simetris modern beroperasi dalam mode *cipher* blok yang merupakan algoritma pengembangan dari algoritma DES (*Data Encryption Standard*). Perbedaan DES dengan Triple DES terletak pada panjangnya kunci yang digunakan. Pada DES menggunakan satu kunci yang panjangnya 56 bit, sedangkan pada Triple DES menggunakan 3 kunci yang panjangnya 168 bit (masing-masing panjangnya 56 bit). Karena tingkat kerahasiaan algoritma *Triple* DES terletak pada panjangnya kunci yang digunakan, maka penggunaan algoritma *Triple* DES dianggap lebih aman dibandingkan dengan algoritma DES (Munir, 2006:149)

2.2.1 DES

DES (*Data Encryption Standard*) adalah algoritma *cipher* blok yang populer karena dijadikan standard algoritma enkripsi kunci-simetri.

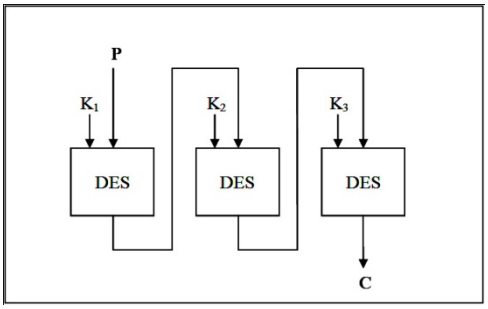


Gambar 1. Jaringan *Feistel* untuk satu putaran DES

Sebenarnya DES adalah nama standard enkripsi simetri, nama algoritma enkripsinya sendiri adalah DEA (*Data Encryption Algorithm*), namun nama DES lebih populer dibandingkan dengan DEA. DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (*subkey*).

2.2.2 Proses Enkripsi

Pada algoritma Triple DES dibagi menjadi tiga tahap, setiap tahapnya merupakan implementasi dari algoritma DES. Triple DES menggunakan tiga buah kunci eksternal, dan tiga buah kunci bisa bersifat saling bebas ($K_1 \neq K_2 \neq K_3$) atau hanya dua buah kunci yang saling bebas, dan kunci yang ketiga sama dengan kunci yang pertama ($K_1 \neq K_2$ dan $K_3 = K_1$).



Gambar 2. Skema algoritma Triple DES

2.2.2 Proses Dekripsi

Proses dekripsi dari cipherteks merupakan kebalikan dari proses enkripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah $k_1,k_2, \ldots k_{16}$ maka pada proses dekripsi, urutan kunci yang digunakan adalah $k_{16}, k_{15}, \ldots k_1$. Blok ($R_{16}$, L_{16}) diperoleh dengan mempermutasikan cipherteks dengan matriks permutasi awal balikan (IP^{-1}). Pra-plainteks dari *deciphering* adalah (R_0, L_0). Dengan mempermutasikan (R_0, L_0) dengan matriks permutasi awal (*IP*), maka akan didapatkan kembali blok plainteks semula. Cara pendekripsian Triple DES bergantung pada mode yang digunakan:

Tabel 1. Mode enkripsi dan dekripsi Triple DES

Enkripsi	**Dekripsi**
TDES – EEE2 $K_1 \neq K_2$ dan $K_3 = K_1$ $C = E_{K1}(E_{K2}(E_{K1}(P)))$	TDES – DDD2 $K_1 \neq K_2$ dan $K_3 = K_1$ $P = D_{K1}(D_{K2}(D_{K1}(C)))$
TDES – EEE3 $K_1 \neq K_2 \neq K_3$ $C = E_{K3}(E_{K2}(E_{K1}(P)))$	TDES – DDD3 $K_1 \neq K_2 \neq K_3$ $P = D_{K1}(D_{K2}(D_{K3}(C)))$
TDES – EDE2 $K_1 \neq K_2$ dan $K_3 = K_1$ $C = E_{K1}(D_{K2}(E_{K1}(P)))$	TDES – DED2 $K_1 \neq K_2$ dan $K_3 = K_1$ $P = D_{K1}(E_{K2}(D_{K1}(C)))$
TDES – EDE3 $K_1 \neq K_2 \neq K_3$ $C = E_{K3}(D_{K2}(E_{K1}(P)))$	TDES – DED3 $K_1 \neq K_2 \neq K_3$ $P = D_{K1}(E_{K2}(D_{K3}(C)))$

2.3 Fungsi *Hash*

Fungsi hash adalah fungsi yang menerima masukan string yang panjangnya sembarang dan mengkonversinya menjadi *string* keluaran yang panjangnya tetap (*fixed*). Fungsi *hash* dapat menerima masukan string apa saja. Jika *string* menyatakan pesan (*message*), maka sembarang pesan *M* berukuran bebas dikompresi oleh fungsi hash *H* melalui persamaan

Keluaran fungsi hash disebut juga nilai hash (*hash-value*) atau pesan-ringkas (*message digest*). Pada persamaan (2.26), *h* adalah nilai hash atau *message digest* dari fungsi *H* untuk masukan *M*. Fungsi hash mengkompresi sembarang pesan yang berukuran berapa saja menjadi *message digest* yang ukurannya selalu tetap.

2.3.1 Fungsi *Hash* Satu-Arah

$h = H(M)$

Fungsi hash satu-arah adalah fungsi *hash* yang bekerja dalam satu arah: pesan yang sudah diubah menjadi *message digest* tidak dapat dikembalikan lagi menjadi pesan semula. Sifat-sifat fungsi hash satu-arah adalah sebagai berikut:

1. Fungsi *H* dapat diterapkan pada blok data berukuran berapa saja.
2. *H* menghasilkan nilai (*h*) dengan panjang tetap (*fixed-length output*).
3. Untuk setiap *h* yang dihasilkan, tidak mungkin mengembalikan nilai *M* sedemikian sehingga $H(M) = h$. Itulah sebabnya fungsi *H* dikatakan fungsi hash satu-arah (*one-way hash function*).

2.4 *Short Message Service* (SMS)

Short Message Services atau disingkat dengan SMS adalah sebuah layanan yang dilaksanakan dengan sebuah telepon seluler atau ponsel untuk mengirim atau menerima pesan-pesan pendek. Pada saat mengirim pesan SMS dari telepon seluler, maka pesan SMS tersebut tidak langsung dikirim ke telepon seluler tujuan, tetapi terlebih dahulu dikirim ke SMS Center (SMSC) dengan prinsip *Store and Forward*, setelah itu baru dikirimkan ke telepon seluler tujuan.

2.5 *Java*

Java adalah bahasa pemrograman yang dapat dijalankan di berbagai komputer termasuk telepon genggam. Bahasa ini awalnya dibuat oleh James Gosling saat masih bergabung di Sun Microsystems Inc dan dirilis tahun 1995. Bahasa pemrograman ini terlahir ketika perusahaan Sun Microsystem memulai *Green Project*, yakni proyek penelitian untuk membuat bahasa yang akan digunakan pada chip-chip *embedded* untuk *customer electronic products*. Java memiliki karakteristik berukuran kecil, efisien dan *portable* untuk berbagai *hardware*. (Nimeyer dan Knudsen, 2005:1-2)

2.6 Extensible Markup Language (XML)

Extensible Markup Language adalah bahasa yang mendefinisikan sekumpulan aturan untuk pengkodean dokumen dalam format yang dapat dibaca oleh manusia (*human-readable*) dan dapat dibaca oleh mesin (*machine-readable*). XML adalah merupakan suatu bahasa *Markup*. *Markup* yaitu bahasa yang berisikan kode-kode berupa tanda-tanda tertentu dengan aturan tertentu untuk memformat dokumen teks dengan tag sendiri agar dapat dimengerti.

2.7 Android

Android adalah sistem operasi yang berbasis Linux dan bersifat open source untuk telepon seluler seperti telepon pintar (*smartphone*) dan komputer tablet yang diciptakan oleh Google dan Open Handset Alliance. Pada saat perilisan perdana Android, 5 November 2007, Android bersama Open Handset Alliance menyatakan mendukung pengembangan standar terbuka pada perangkat seluler. Di lain pihak, Google merilis kode-kode Android di bawah lisensi Apache, sebuah lisensi perangkat lunak dan standar terbuka perangkat seluler. (Brunette, 2010:10).

2.8 Metodologi Rekayasa Perangkat Lunak

Model proses perangkat lunak merupakan deskripsi yang disederhanakan dari proses perangkat lunak yang dipresentasikan dengan sudut pandang tertentu. Jenis pemodelan yang digunakan dalam penyelesaian tugas akhir ini menggunakan pemodelan yang secara umum digunakan dalam rekayasa perangkat lunak yaitu model sekuensial linier atau sering disebut juga model *waterfall*.

Model *waterfall* mengusulkan sebuah pendekatan kepada perkembangan perangkat lunak yang sistematik dan sekuensial yang mulai pada tingkat dan kemajuan sistem pada seluruh analisis, desain, kode, pengujian, dan pemeliharaan (Pressman, 2007).

2.9 *Unified Modelling Language*

UML merupakan keluarga notasi grafis yang didukung oleh meta-model tunggal, yang membantu pendeksripsian dan desain sistem perangkat lunak, khususnya sistem yang dibangun menggunakan pemograman berorientasi objek (Fowler, 2003). UML juga merupakan suatu metode terbuka yang digunakan untuk menspesifikasi, memvisualisasi, membangun dan mendokumentasikan artifak-artifak dari suatu pengembangan sistem perangkat lunak yang berbasis pada objek. UML sudah menjadi standar industri yang dibuat dibawah pengawasan *Object Management Group* (OMG) (Weilkiens, 2006:143).

3. ANALISIS DAN PERANCANGAN

3.1 Analisis Kebutuhan

Faktor yang mendasari dibentuknya perangkat lunak dengan algoritma Triple DES ini adalah keamanan data. Keamanan data telah menjadi aspek yang sangat penting dari suatu sistem informasi. Sebuah informasi umumnya hanya ditujukan bagi segolongan tertentu. Oleh karena itu sangatlah penting untuk mencegahnya agar tidak jatuh kepada pihak-pihak yang tidak berhak. Untuk keperluan tersebut, maka diperlukan sebuah teknik kriptografi dengan metode enkripsi dan dekripsi pesan dengan memanfaatkan algoritma kriptografi Triple DES. Perangkat lunak ini diberi nama "*Crypto Messenger*".

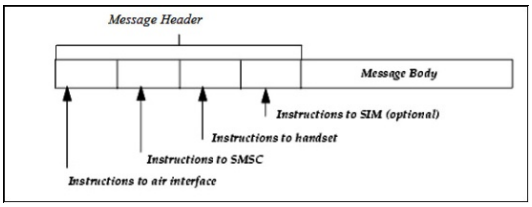
Secara teknis, aplikasi yang akan dibangun memiliki fungsionalitas sebagai berikut:

1. Memiliki kemampuan untuk mengirimkan dan menerima pesan melalui SMS.
2. Memiliki kemampuan untuk melakukan proses enkripsi dan dekripsi pesan dengan menggunakan algoritma Triple DES tiga kunci.
3. Memiliki kemampuan untuk membuka daftar kontak pada telepon seluler.

4. Memiliki kemampuan untuk mengakses kotak masuk pesan telepon seluler.

3.2 Analisis Struktur Pesan SMS

Secara teknis pengiriman pesan SMS dilakukan dengan menggunakan struktur seperti yang dapat dilihat dalam gambar berikut ini:



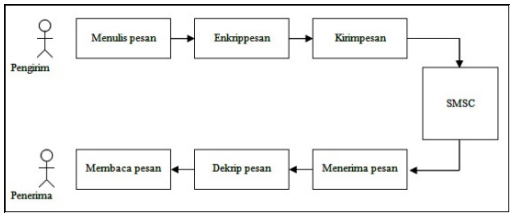
Gambar 3. Struktur pesan SMS

Pada gambar di atas dapat dilihat bahwa pada sebuah paket pesan SMS sebenarnya terdiri dari dua bagian besar. Bagian pertama disebut dengan *Header* yang terdiri atas instruksi-instruksi kepada komponen-komponen yang bekerja dalam jaringan SMS. Instruksi yang dikirimkan adalah informasi yang diperlukan untuk mengirimkan pesan seperti informasi validitas pesan, informasi nomor tujuan, serta informasi lainnya. Bagian kedua disebut *Body* yaitu berisikan pesan yang dikirimkan oleh pengguna.

Perlu diperhatikan pada *Header* terdiri dari instruksi-instruksi kepada komponen-komponen jaringan SMS, sehingga apabila terjadi kehilangan data atau kerusakan data pada bagian *Header* ini, maka akan berakibat pada kegagalan pengiriman pesan tersebut. Sebagai contoh, apabila kita melakukan enkripsi pada bagian *Header*, dimana kita melakukan proses enkripsi terhadap nomor tujuan dari pesan tersebut, maka yang terjadi adalah nomor tujuan dari pesan tersebut tidak akan dikenali oleh operator sehingga pesan tersebut gagal dalam proses pengiriman pesan. Tentu saja hal ini merupakan hal yang tidak diinginkan oleh pengguna. Agar pesan dapat dikirimkan dengan baik, maka dalam melakukan proses enkripsi adalah hanya pada bagian *Body* saja.

3.3 Analisis Sistem

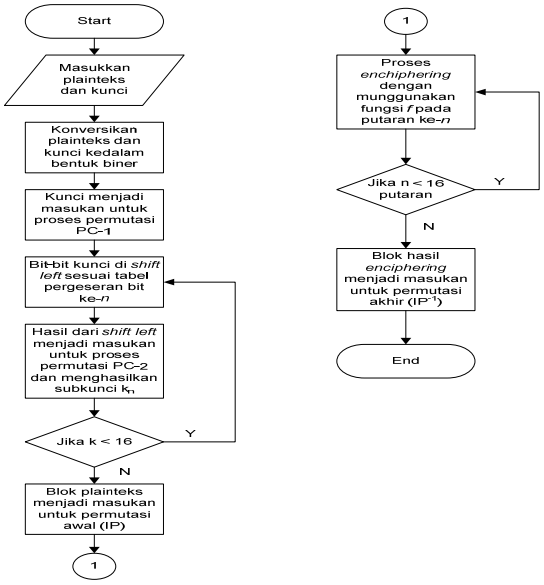
Tahapan analisis terhadap suatu sistem dilakukan sebelum tahapan perancangan dilakukan. Adapun tujuan dilakukannya analisis terhadap suatu sistem adalah untuk mendapatkan pemahaman secara keseluruhan tentang sistem yang akan dibuat berdasarkan masukan dari pihak-pihak yang berkepentingan dengan sistem tersebut. Cara kerja sistem ini dibagi ke dalam beberapa proses utama, yaitu sebagai berikut:



Gambar 4. Arsitektur sistem

3.4 Analisis Algoritma

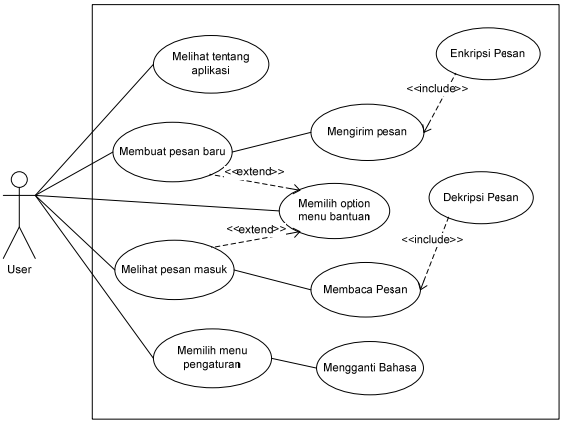
Triple DES atau TDES merupakan algoritma kriptografi yang menggunakan tiga kali algoritma DES. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (*subkey*). Berikut ini merupakan alur kerja dari algoritma DES ditampilkan dalam bentuk diagram alir (*flowchart*):



Gambar 5. Diagram alir algoritma DES

3.5 Pemodelan *Use Case Diagram*

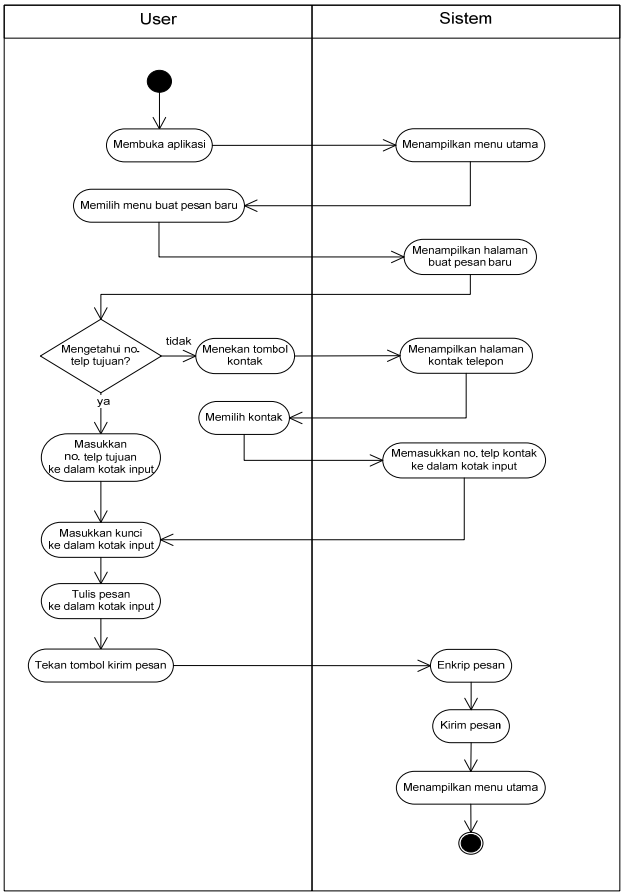
Use case diagram digunakan untuk menjelaskan dan menggambarkan pengguna sistem dan perilaku pengguna terhadap sistem. *Use case diagram* menekankan tentang apa yangakan diperbuat oleh sistem dan bukan menekankan bagaimana sistem tersebut bertindak. Pengguna sistem diwakili oleh aktor, sedangkan perilakunya diwakili oleh *use case*.



Gambar 6. Use case diagram aplikasi Crypto Messenger

3.6 Pemodelan *Activity Diagram*

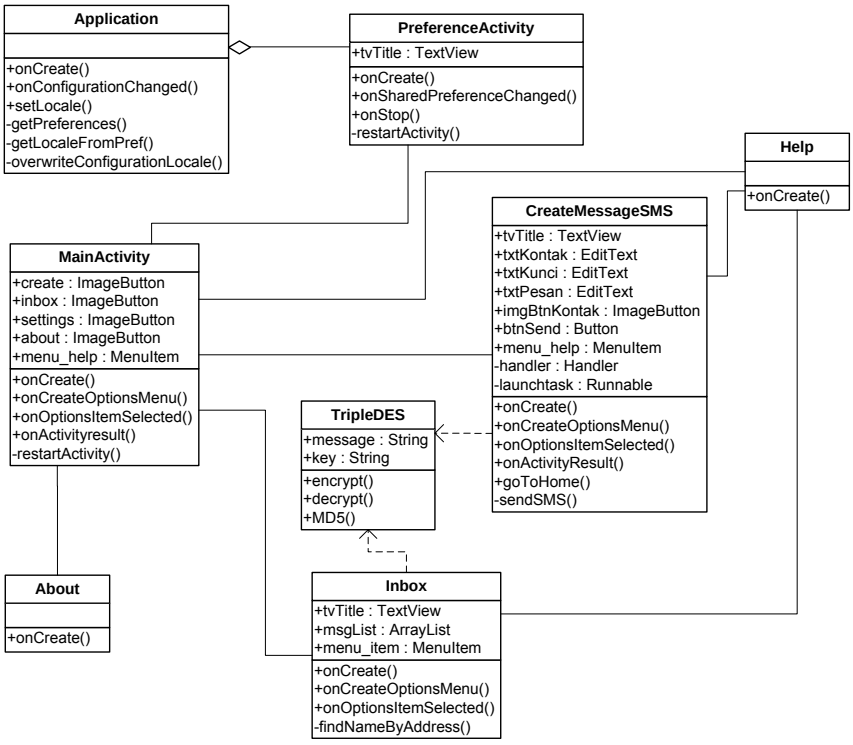
Diagram *activity* berikut ini menjelaskan interaksi antara *user* dan sistem ketika membuat pesan baru.



Gambar 7. Activity diagram membuat pesan baru

3.7 Pemodelan *Class Diagram*

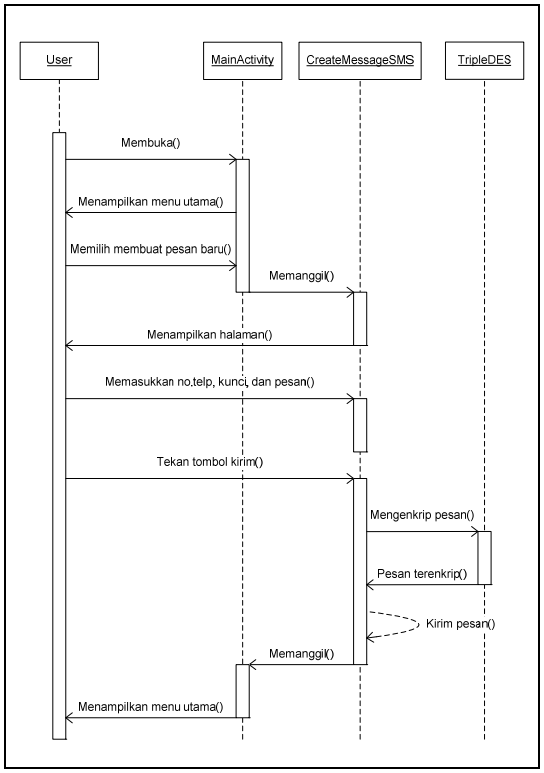
Class diagram merupakan diagram yang menggambarkan struktur dan penjelasan kelas, paket, dan objek serta hubungan satu sama lain seperti pewarisan, asosiasi, dan lain-lain.



Gambar 8. *Class diagram* aplikasi *Crypto Messenger*

3.8 Pemodelan *Sequence Diagram*

Sequence diagram menggambarkan interaksi antar objek didalam dan di sekitar sistem (termasuk *user*, *display* dan sebagainya) berupa *message* yang digambarkan terhadap waktu.



Gambar 9. Sequence Diagram membuat pesan baru

Sequence diagram terdiri atas dimensi vertikal (waktu) dan dimensi horizontal (objek-objek yang terkait).

4. IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi Program dan Antarmuka

Tampilan pertama kali yang muncul ketika aplikasi dijalankan adalah halaman Menu Utama. Menu Utama aplikasi menampilkan menu untuk mengirim pesan, melihat kotak masuk, pengaturan, dan tentang aplikasi.

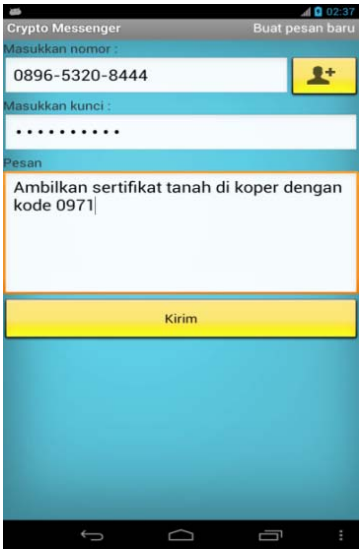
4.1.1 Menampilkan Menu Utama

Saat pertama kali aplikasi *Crypto Messenger* dijalankan, aplikasi akan menampilkan halaman menu utama. Tampilan antarmuka halaman menu utama terdapat beberapa pilihan menu dimana pengguna bisa memilih layanan yang ditampilkan pada aplikasi.

Gambar 10. Tampilan antarmuka halaman menu utama

4.1.2 Mengenkripsi dan Mengirim Pesan

Saat memilih menu membuat pesan baru, maka aplikasi akan menampilkan halaman untuk menulis pesan. Antarmuka halaman Buat pesan baru terdiri dari sebuah *text field* untuk memasukkan nomor tujuan, sebuah *text field* untuk memasukkan kunci, dan sebuah *text field* untuk menulis pesan.



Gambar 11. Tampilan antarmuka halaman buat pesan baru

4.1.3 Mendekripsi dan Menampilkan Pesan

Gambar 12. Tampilan antarmuka halaman buat pesan baru

Saat memilih menu kotak masuk, maka aplikasi akan menampilkan halaman yang berisi pesan-pesan yang tersimpan di kotak masuk telepon seluler.

4.2 Pengujian Aplikasi

Pengujian ini dilakukan agar diketahui apakah aplikasi dapat berjalan sesuai dengan kebutuhan.

4.2.1 Pengujian Enkripsi dan Dekripsi

Pengujian enkripsi dan dekripsi ini bertujuan untuk mengetahui apakah proses enkripsi dan dekripsi ini sudah sesuai dengan apa yang diharapkan. Dalam pengujian ini dicoba apakah hasil dari enkripsi dapat didekripsikan kembali dan menampilkan isi dari pesan tersebut dengan utuh atau tidak.

Tabel 2. Pengujian enkripsi pesan

Plainteks	Jumlah karakter	Kunci	Cipherteks	Jumlah karakter
hello	5	password	9c2bada78dc460b1	16
beruang	7	qwertyui	ec3c6c582305c04c	16
kurakura	8	password	c759742630a33a438824b88c6321aa85	32
mercubuana	10	abcdefgh	3037f5f782faf5a44bd17d592385e84e	32
mercubuana	10	b	2367495eac7527637ce68edac4e310d6	32
univ.mercubuana	15	umb	42c409530c13f11b0f5912d625319cbc	32
M. Rival. Suheri	16	umb	0c554a26a6cdfc9df40051659a27db6e 38ad8afb55ce36d5	48

Tabel 3. Pengujian dekripsi pesan

Cipherteks	Jumlah karakter	Kunci	Plainteks	Jumlah karakter
9c2bada78dc460b1	16	password	hello	5
ec3c6c582305c04c	16	qwertyui	beruang	7
c759742630a33a438824b88c6321aa85	32	password	kurakura	8
3037f5f782faf5a44bd17d592385e84e	32	abcdefgh	mercubuana	10
2367495eac7527637ce68edac4e310d6	32	b	mercubuana	10
42c409530c13f11b0f5912d625319cbc	32	umb	univ.mercubuana	15
0c554a26a6cdfc9df40051659a27db6e 38ad8afb55ce36d5	48	umb	M. Rival. Suheri	16

4.3 Analisis Hasil Pengujian

Analisis hasil pengujian dari aplikasi ini menunjukkan bahwa hasil pencapaian aplikasi dan fungsi sudah berjalan lancar dan sesuai dengan rancangan aplikasi program. Dari hasil pengujian dapat dijelaskan sebagai berikut:

1. Aplikasi dapat dijalankan pada versi 2.2 (Froyo) sampai dengan 4.2 (Jelly Bean).
2. Aplikasi dapat menampilkan halaman kontak nomor telepon pada kontak telepon seluler.
3. Aplikasi dapat mengenkripsi pesan dan mengirimkan *cipherteks* melalui layanan SMS
4. Tombol-tombol yang ada pada aplikasi dapat berfungsi dengan baik dan sesuai yang diharapkan.

5. Aplikasi dapat menampilkan pesan yang tersimpan pada kotak masuk telepon seluler
6. Aplikasi dapat mendekripsikan pesan jika memasukkan kunci yang tepat dan menampilkannya dengan baik.
7. Aplikasi dapat menampilkan bahasa antarmuka aplikasi sesuai dengan pilihan pengguna.
8. *Cipherteks* yang dihasilkan dari proses pengenkripsian pesan berupa *string.*
9. heksadesimal yang tidak bisa dibaca oleh manusia.

5. PENUTUP

5.1 Kesimpulan

Selama proses implementasi dan pengujian yang dilakukan penulis terhadap aplikasi enkripsi SMS dengan algoritma Triple DES ini, penulis mengambil kesimpulan sebagai berikut:

1. Dengan adanya aplikasi enkripsi SMS dengan algoritma Triple DES ini pengguna bisa menggunakan layanan SMS dan dapat bertukar informasi dengan aman tanpa takut diketahui oleh pihak yang tidak berhak. Pesan yang terenkripsi tidak akan dapat dibaca jika tidak didekripsi dengan kunci yang benar, sehingga orang yang tidak mengetahui kunci yang benar tidak dapat membaca pesan.
2. Algoritma Triple DES dapat diimplementasi-kan untuk melakukan enkripsi dan dekripsi pesan SMS pada telepon seluler bersistem operasi Android.
3. Aplikasi ini mampu berjalan dengan baik pada *platform* Android yang bersistem operasi versi 2.2 (Froyo) sampai 4.2 (Jellybean) dimana mungkin ada sedikit perbedaan pada tampilan aplikasi di setiap jenis telepon seluler karena setiap telepon seluler memiliki resolusi layar yang berbeda-beda
4. Pesan yang dikirimkan menjadi lebih besar karena bekerja pada blok-blok 8-bit dan dibutuhkan *padding* untuk memenuhi panjang blok.

5.2 Saran

Dari uraian diatas, penulis memberikan saran yang untuk pengembangan lebih lanjut antara lain:

1. Aplikasi mendukung untuk dapat terintegrasi ke *instant messenger* (IM) seperti Facebook Messenger, Yahoo! Messenger, Google Talk, MSN dan yang lainnya.
2. Aplikasi dapat mendukung ke berbagai *platform* yang berbeda seperti Blackberry, iOS dan Windows phone.
3. Aplikasi dapat menampilkan pesan masuk dan keluar dalam bentuk *threaded view* seperti aplikasi SMS bawaan android.
4. Agar pesan terenkripsi yang dikirimkan memiliki panjang pesan yang sama atau lebih kecil dengan plainteks, dapat diterapkan sebuah algoritma kompresi untuk melakukan kompresi pesan yang dikirimkan.

6. DAFTAR PUSTAKA

A.S, Rosa dan M. Shalahuddin. 2011. *Modul Pembelajaran Rekayasa Perangkat Lunak - Terstruktur dan Berorientasi Objek.* Bandung: Modula

Android Developers. Localization. (http://developer.android.com/guide/topics/resources/localization.html, diakses pada tanggal 16 Desember 2012)

-------. Menus. (http://developer.android.com/guide/topics/ui/menus.html, diakses pada tanggal 12 Desember 2012)

-------. Supporting Different Language. (http://developer.android.com/training/basics/supporting-devices /languages.html, diakses pada tanggal 16 Desember 2012)

Brunette, Ed. 2010. *Hello, Android - Introducing Google's Mobile Development Platform, 3rd Edition*. North Carolina: The Pragmatic Bookshelf

Dexter, M. 2007. *Eclipse And Java for Total Beginners*. Tutorial Companion Document

Fowler, M. 2003. *UML Distilled: A Breaf Guide to the Standard Object Modelling Language, Third Edition*. Boston: Addison-Wesley

Global System for Mobile Communications. (http://en.wiki pedia.org/wiki/GSM, diakses pada tanggal 15 November 2012)

Lee, Wei-Meng. 2011. *Beginning Android™ Application Development.* Indianapolis: Wiley Publishing

Meier, R. 2009. *Professional Android™ Application Development*. Indianapolis: Wiley Publishing

Munir, R. 2006. *Kriptografi*. Bandung: Informatika.

Nimeyer, P dan Jonathan Knudsen. 2005. *Learning Java*. CA: O'Reilly Media

Pressman, R.S. 2005. *Software Engineering: A Practitioner's Approach, Fifth Edition.* Boston: McGraw-Hill

Sadikin, R. 2012. *Kriptografi untuk Keamanan Jaringan*. Yogyakarta: Penerbit Andi

Stallings, W. 2011. *Cryptography and Network Security: Principles and Practice, Fifth Edition*. Boston: Pearson Education